FINITE FIELDS AND THEIR APPLICATIONS **3,** 203–218 (1997)
ARTICLE NO. FF970180

Average Discrepancy, Hyperplanes, and Compound Pseudorandom Numbers

Jürgen Eichenauer-Herrmann and Frank Emmerich

Fachbereich Mathematik, Technische Hochschule, Schloßgartenstraße 7, D-64289

similar papers at core.ac.uk

and

Gerhard Larcher

Institut für Mathematik, Universität Salzburg, Hellbrunner Straße 34, A-5020 Salzburg, Austria
E-mail: Gerhard.Larcher@sbg.ac.at

Communicated by Harald Niederreiter

Received August 6, 1996; revised December 30, 1996

This paper deals with compound nonlinear congruential methods for generating uniform pseudorandom numbers. The average equidistribution and statistical independence behavior of the generated sequences over arbitrary parts of the period is studied, based on the average value of the discrepancy of certain point sets. General upper bounds for these average values are established, which depend on the number of points on certain hyperplanes over finite fields. These bounds are applied to the compound explicit inversive congruential method, which has been introduced recently. © 1997 Academic Press

1. INTRODUCTION

Nonlinear methods of generating uniform pseudorandom numbers in the interval [0, 1) have been studied intensively during the last 10 years. The development of this attractive field of research is described in the survey articles [2, 3, 9, 15, 16, 19, 20, 22] and in the excellent monograph of Niederreiter [18]. Recently, compound versions of these methods, which show several computational advantages, have been introduced and analyzed

1071-5797/97 $25.00
Copyright © 1997 by Academic Press
All rights of reproduction in any form reserved.

[5–8, 10–13]. It turned out that, over the full period and over large parts of the period, the generated sequences of compound pseudorandom numbers have nice equidistribution and statistical independence properties. The present paper deals with the average behavior of these pseudorandom numbers over arbitrary parts of the period. The following general compound approach is studied.

Let $p_1, \ldots, p_r$ be arbitrary distinct primes. For $1 \le i \le r$, identify the set $\mathbb{Z}_{p_i} = \{0, 1, \ldots, p_i - 1\}$ with the finite field of order p_i, and let $\mathbb{Z}_{p_i}^* = \mathbb{Z}_{p_i} \setminus \{0\}$ be its multiplicative group. Let $(\mathbf{z}_n^{(i)})_{n \ge 0}$ be a sequence of elements of $\mathbb{Z}_{p_i}^s$, which is purely periodic with period length p_i. For a *parameter* $c_i \in \mathbb{Z}_{p_i}^*$, let $(\mathbf{x}_n^{(i)})_{n \ge 0}$ with

$$\mathbf{x}_n^{(i)} \equiv c_i \mathbf{z}_n^{(i)} / p_i \pmod 1, \quad n \ge 0,$$

be the corresponding stream of s-dimensional vectors of (ordinary) *pseudorandom numbers* in the interval $[0, 1)$. A sequence $(\mathbf{x}_n)_{n \ge 0}$ of s-dimensional vectors of *compound pseudorandom numbers* in the interval $[0, 1)$ is defined by

$$\mathbf{x}_n \equiv \mathbf{x}_n^{(1)} + \cdots + \mathbf{x}_n^{(r)} \pmod 1, \quad n \ge 0.$$

Since the primes $p_1, \ldots, p_r$ are distinct, it follows by standard arguments that the sequence $(\mathbf{x}_n)_{n \ge 0}$ is purely periodic with period length $m = p_1 \cdots p_r$. It should be observed that in the compound approach a very large period length m and an excellent discretization $1/m$ can be obtained, although exact integer computations have to be performed only in the finite fields $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}$. Additionally, compound methods are particularly suitable for parallelized computations, since the underlying sequences $(\mathbf{x}_n^{(i)})_{n \ge 0}$ can be computed by parallel processors.

Equidistribution and statistical independence properties of uniform pseudorandom numbers, which are very important for their usability in stochastic simulations, can be analyzed based on the discrepancy of certain point sets in $[0, 1)^s$. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^s$, the *discrepancy* is defined by

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^s$, $F_N(J)$ is N^{-1} times the number of points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the s-dimensional volume of J.

In the following, the s-dimensional vectors $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{m-1}$ of compound pseudorandom numbers are considered and the abbreviation

$$D^{(s)}_{N;c_1,\ldots,c_r} = D_N(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1})$$

is used for $1 \le N \le m$. In the third section, upper bounds for the average value of the discrepancy $D^{(s)}_{N;c_1,\ldots,c_r}$ over the parameters $c_1, \ldots, c_r$ are established. These bounds only depend on the number of points among $\mathbf{z}_0^{(i)}, \mathbf{z}_1^{(i)}, \ldots, \mathbf{z}_{p_i-1}^{(i)}$ falling into certain hyperplanes over the finite field $\mathbb{Z}_{p_i}$. In the fourth section, these general results are applied to the compound explicit inversive congruential method. The second section contains necessary auxiliary results.

2. AUXILIARY RESULTS

First, some further notation is necessary. For integers $k \ge 1$ and $q \ge 2$, let $C_k(q)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbb{Z}^k$ with $-q/2 < h_j \le q/2$ for $1 \le j \le k$. Define

$$r(h,q) = \begin{cases} q \sin(\pi|h|/q) & \text{for } h \in C_1(q), \\ 1 & \text{for } h = 0, \end{cases}$$

and

$$r(\mathbf{h}, q) = \prod_{j=1}^{k} r(h_j, q)$$

for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(q)$. For real t, the abbreviation $e(t) = e^{2\pi i t}$ is used, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$. Subsequently, three known results are stated, which follow from [18, Theorem 3.10, Corollary 3.17] and [8, Lemma 3], respectively.

LEMMA 1. *Let $N \ge 1$ and $q \ge 2$ be integers. Let $\mathbf{t}_n = \mathbf{y}_n/q \in [0,1)^k$ with $\mathbf{y}_n \in \{0, 1, \ldots, q-1\}^k$ for $0 \le n < N$. Then the discrepancy of the points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ satisfies*

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) \le \frac{k}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_k(q)} \frac{1}{r(\mathbf{h}, q)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right|.$$

LEMMA 2. *The discrepancy of N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0,1)^k$ satisfies*

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) \ge \frac{\pi}{2N((\pi+1)^\ell - 1) \prod_{j=1}^{k} \max(1, |h_j|)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right|$$

for any nonzero lattice point $\mathbf{h} = (h_1, \ldots, h_k) \in \mathbb{Z}^k$, *where* ℓ *denotes the number of nonzero coordinates of* $\mathbf{h}$.

LEMMA 3. *Let* $q \geq 2$ *be an integer. Then*

$$\sum_{\substack{\mathbf{h} \in C_k(q) \\ \mathbf{h} \equiv \mathbf{0} (\mathrm{mod} d)}} \frac{1}{r(\mathbf{h}, q)} < \frac{1}{d} \left(\frac{2}{\pi} \log q + \frac{7}{5} \right)^k$$

for any divisor d *of* q *with* $1 \leq d < q$.

The following quantities play a crucial role for the analysis of the average discrepancy. For $1 \leq i \leq r$ and $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$, define

$$A_i(\mathbf{h}) = \frac{1}{p_i} \sum_{h_0 \in \mathbb{Z}_{p_i}} (\#\{0 \leq n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv h_0 \pmod{p_i}\})^2$$

and

$$B_i(\mathbf{h}) = \max_{h_0 \in \mathbb{Z}_{p_i}} \#\{0 \leq n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv h_0 \pmod{p_i}\};$$

i.e., for fixed $\mathbf{h} = (h_1, \ldots, h_s)$, the quantity $A_i(\mathbf{h})$ is the average value (in the mean-square sense) of the number of points $\mathbf{z}_0^{(i)}, \mathbf{z}_1^{(i)}, \ldots, \mathbf{z}_{p_i-1}^{(i)}$ lying on one of the parallel hyperplanes

$$H = \{(z_1, \ldots, z_s) \in \mathbb{Z}_{p_i}^s \mid h_1 z_1 + \cdots + h_s z_s \equiv h_0 \pmod{p_i}\}, h_0 \in \mathbb{Z}_{p_i},$$

and any of the hyperplanes H contains at most $B_i(\mathbf{h})$ of these points. It should be observed that

$$1 \leq A_i(\mathbf{h}) \leq B_i(\mathbf{h}) \leq p_i,$$

since any point lies on exactly one hyperplane.

LEMMA 4. *Let* $1 \leq N \leq m$, $\mathbf{h} \in C_s(m)$, *and* $J = \{1 \leq i \leq r \mid \mathbf{h} \equiv \mathbf{0} \pmod{p_i}\}$. *Then*

$$\sum_{(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)}) / p_i \right) \right|^2 \leq Nm \prod_{i \in J} p_i \prod_{\substack{i=1 \\ i \notin J}}^{r} B_i(\mathbf{h}).$$

Proof. Straightforward calculations show that

$$\begin{aligned}
&\sum_{(c_1,\dots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2\\
&\quad\le \sum_{(c_1,\dots,c_r)\in\mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}}\left|\sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2\\
&\quad= \sum_{(c_1,\dots,c_r)\in\mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}}\sum_{k,n=0}^{N-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)}-\mathbf{h}\cdot\mathbf{z}_k^{(i)})/p_i\right)\\
&\quad= \sum_{k,n=0}^{N-1}\sum_{(c_1,\dots,c_r)\in\mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}}\prod_{i=1}^{r} e\left(c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)}-\mathbf{h}\cdot\mathbf{z}_k^{(i)})/p_i\right)\\
&\quad= \sum_{k,n=0}^{N-1}\prod_{i=1}^{r}\sum_{c\in\mathbb{Z}_{p_i}} e(c(\mathbf{h}\cdot\mathbf{z}_n^{(i)}-\mathbf{h}\cdot\mathbf{z}_k^{(i)})/p_i)\\
&\quad= m\sum_{k=0}^{N-1}\#\{0\le n<N \mid \mathbf{h}\cdot\mathbf{z}_n^{(i)}\equiv\mathbf{h}\cdot\mathbf{z}_k^{(i)}\ (\mathrm{mod}\ p_i), 1\le i\le r\}\\
&\quad\le m\sum_{k=0}^{N-1}\#\{0\le n<m \mid \mathbf{h}\cdot\mathbf{z}_n^{(i)}\equiv\mathbf{h}\cdot\mathbf{z}_k^{(i)}\ (\mathrm{mod}\ p_i), 1\le i\le r\}\\
&\quad= m\sum_{k=0}^{N-1}\prod_{i=1}^{r}\#\{0\le n<p_i \mid \mathbf{h}\cdot\mathbf{z}_n^{(i)}\equiv\mathbf{h}\cdot\mathbf{z}_k^{(i)}\ (\mathrm{mod}\ p_i)\},
\end{aligned}$$

where in the last step the periodicity properties of the sequences $(\mathbf{z}_n^{(i)})_{n\ge0}$ and the Chinese Remainder Theorem were used. Hence, it follows that

$$\sum_{(c_1,\dots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2 \le Nm\prod_{i\in J} p_i\prod_{\substack{i=1\\ i\notin J}}^{r} B_i(\mathbf{h}),$$

which is the desired result. ■

LEMMA 5. *Let* $\mathbf{h}\in C_s(m)$ *and* $J=\{1\le i\le r \mid \mathbf{h}\equiv\mathbf{0}\ (\mathrm{mod}\ p_i)\}$. *Then*

$$\sum_{(c_1,\dots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{m-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2 = m^2\prod_{i\in J}(p_i-1)\prod_{\substack{i=1\\ i\notin J}}^{r}(A_i(\mathbf{h})-1).$$

Proof. First, the Chinese Remainder Theorem and the periodicity properties of the sequences $(\mathbf{z}_n^{(i)})_{n\ge 0}$ imply that

$$\sum_{n=0}^{m-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right) = \sum_{n=0}^{m-1}\prod_{i=1}^{r} e\left(c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right) = \prod_{i=1}^{r}\sum_{n=0}^{p_i-1} e\left(c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)$$

for all $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$. Hence, a short calculation shows that

$$\sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} \left|\sum_{n=0}^{m-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2 = \prod_{i=1}^{r}\sum_{c\in\mathbb{Z}_{p_i}^*}\left|\sum_{n=0}^{p_i-1} e\left(c(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2$$

$$= \prod_{i=1}^{r}\left(\sum_{k,n=0}^{p_i-1}\sum_{c\in\mathbb{Z}_{p_i}} e(c(\mathbf{h}\cdot\mathbf{z}_n^{(i)} - \mathbf{h}\cdot\mathbf{z}_k^{(i)})/p_i) - p_i^2\right)$$

$$= m^2\prod_{i=1}^{r}\left(\frac{1}{p_i}\#\{(k,n)\in\mathbb{Z}_{p_i}^2 \mid \mathbf{h}\cdot\mathbf{z}_n^{(i)} \equiv \mathbf{h}\cdot\mathbf{z}_k^{(i)} \pmod{p_i}\} - 1\right)$$

$$= m^2\prod_{i\in J}(p_i - 1)\prod_{\substack{i=1\\ i\notin J}}^{r}(A_i(\mathbf{h}) - 1),$$

which is the desired result. ∎

3. DISCREPANCY BOUNDS

In Theorems 1 and 2, upper bounds for the average value of the discrepancy of s-dimensional vectors in the compound method both over the full period ($N = m$) and over parts of the period ($N < m$) are established, which only depend on the quantities $B_i(\mathbf{h})$ defined above. In the full period case ($N = m$), these bounds are improved quite a bit in Theorems 3 and 4 by using the quantities $A_i(\mathbf{h})$ instead of $B_i(\mathbf{h})$. Finally, lower bounds for the discrepancy over the full period ($N = m$) are given in Theorems 5 and 6, which also depend on the quantities $A_i(\mathbf{h})$. In particular, Theorem 6 shows that there exist sequences of s-dimensional vectors in the compound method with a discrepancy over the full period which is relatively large compared with the upper bound for the corresponding average value in Theorem 4. In this sense, the result of Theorem 4 is essentially best possible. In the following, let $m_J = \prod_{i\in J} p_i$ for subsets J of $\{1, \ldots, r\}$.

THEOREM 1. *Let $1 \le N \le m$. Then the average value of the discrepancy $D_{N;c_1,\ldots,c_r}^{(s)}$ of s-dimensional vectors in the compound method over the parameters $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ satisfies*

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)}$$

$$\le \frac{s}{m}+\frac{1}{\sqrt{N}}\prod_{i=1}^{r}\sqrt{\frac{p_i}{p_i-1}}\sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}}\sqrt{m_J}\sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\ p_i),i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\ p_i),i\notin J}}\frac{1}{r(\mathbf{h},m)}\prod_{\substack{i=1\\ i\notin J}}^{r}\sqrt{B_i(\mathbf{h})}.$$

Proof. First, Lemma 1 is applied with $k=s$, $q=m$, and $\mathbf{t}_n=\mathbf{x}_n$ for $0\le n<N$. This yields

$$D_{N;c_1,\ldots,c_r}^{(s)} \le \frac{s}{m}+\frac{1}{N}\sum_{\mathbf{h}\in C_s(m)}\frac{1}{r(\mathbf{h},m)}\left|\sum_{n=0}^{N-1}e(\mathbf{h}\cdot\mathbf{x}_n)\right|$$

$$=\frac{s}{m}+\frac{1}{N}\sum_{\mathbf{h}\in C_s(m)}\frac{1}{r(\mathbf{h},m)}\left|\sum_{n=0}^{N-1}e\left(\sum_{i=1}^{r}c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|$$

for any $(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*$. Therefore, the average value of the discrepancy $D_{N;c_1,\ldots,c_r}^{(s)}$ over $(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*$ satisfies

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)} \le \frac{s}{m}+\frac{1}{N}\sum_{\mathbf{h}\in C_s(m)}\frac{1}{r(\mathbf{h},m)}$$

$$\times\left(\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(\sum_{i=1}^{r}c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|\right)$$

$$\le\frac{s}{m}+\frac{1}{N}\sum_{\mathbf{h}\in C_s(m)}\frac{1}{r(\mathbf{h},m)}$$

$$\times\sqrt{\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(\sum_{i=1}^{r}c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2}$$

$$=\frac{s}{m}+\frac{1}{N}\sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}}\sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\ p_i),i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\ p_i),i\notin J}}\frac{1}{r(\mathbf{h},m)}$$

$$\times\sqrt{\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(\sum_{i=1}^{r}c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i\right)\right|^2},$$

where the penultimate step follows from the Cauchy–Schwarz inequality. Now, Lemma 4 can be used in order to obtain

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)} \\
&\quad \le \frac{s}{m} + \frac{1}{N} \sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}} \sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\, p_i), i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\, p_i), i\notin J}} \frac{1}{r(\mathbf{h},m)} \sqrt{\frac{Nm}{\prod_{i=1}^{r}(p_i-1)} \prod_{i\in J} p_i \prod_{\substack{i=1\\ i\notin J}}^{r} B_i(\mathbf{h})} \\
&\quad = \frac{s}{m} + \frac{1}{\sqrt{N}} \prod_{i=1}^{r} \sqrt{\frac{p_i}{p_i-1}} \sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}} \sqrt{m_J} \sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\, p_i), i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\, p_i), i\notin J}} \frac{1}{r(\mathbf{h},m)} \prod_{\substack{i=1\\ i\notin J}}^{r} \sqrt{B_i(\mathbf{h})},
\end{aligned}$$

which is the desired result. ■

THEOREM 2. *Let* $1 \le N \le m$ *and* $B_i = \max\{B_i(\mathbf{h}) \mid \mathbf{h} \in \mathbb{Z}^s, \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}\}$ *for* $1 \le i \le r$. *Then the average value of the discrepancy* $D_{N;c_1,\ldots,c_r}^{(s)}$ *of s-dimensional vectors in the compound method over the parameters* $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ *satisfies*

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)} < \frac{1}{\sqrt{N}} \prod_{i=1}^{r} \frac{\sqrt{p_i B_i}+1}{\sqrt{p_i-1}} \left(\frac{2}{\pi}\log m + \frac{7}{5}\right)^s.$$

Proof. First, Theorem 1 implies that

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)} \\
&\quad \le \frac{s}{m} + \frac{1}{\sqrt{N}} \prod_{i=1}^{r} \sqrt{\frac{p_i}{p_i-1}} \sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}} \sqrt{m_J} \sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\, p_i), i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\, p_i), i\notin J}} \frac{1}{r(\mathbf{h},m)} \prod_{\substack{i=1\\ i\notin J}}^{r} \sqrt{B_i} \\
&\quad \le \frac{s}{m} + \frac{1}{\sqrt{N}} \prod_{i=1}^{r} \sqrt{\frac{p_i}{p_i-1}} \sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}} \sqrt{m_J} \sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{1}(\mathrm{mod}\, m_J)}} \frac{1}{r(\mathbf{h},m)} \prod_{\substack{i=1\\ i\notin J}}^{r} \sqrt{B_i}.
\end{aligned}$$

Hence, it follows from Lemma 3 that

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)}\\
&\quad<\frac{s}{m}+\frac{1}{\sqrt{N}}\prod_{i=1}^{r}\sqrt{\frac{p_i}{p_i-1}}\sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}}\frac{1}{\sqrt{m_J}}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^s\prod_{\substack{i=1\\ i\notin J}}^{r}\sqrt{B_i}\\
&\quad<\frac{1}{\sqrt{N}}\prod_{i=1}^{r}\sqrt{\frac{p_i}{p_i-1}}\sum_{J\subset\{1,\ldots,r\}}\prod_{i\in J}\frac{1}{\sqrt{p_i}}\prod_{\substack{i=1\\ i\notin J}}^{r}\sqrt{B_i}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^s\\
&\quad=\frac{1}{\sqrt{N}}\prod_{i=1}^{r}\sqrt{\frac{p_i}{p_i-1}}\prod_{i=1}^{r}\left(\frac{1}{\sqrt{p_i}}+\sqrt{B_i}\right)\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^s\\
&\quad=\frac{1}{\sqrt{N}}\prod_{i=1}^{r}\frac{\sqrt{p_iB_i}+1}{\sqrt{p_i-1}}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^s,
\end{aligned}$$

which is the desired result. ■

Remark. The general upper bounds for the average value of the discrepancy $D_{N;c_1,\ldots,c_r}^{(s)}$ in Theorems 1 and 2, both over parts of the period ($N < m$) and over the full period ($N = m$), cannot be best possible in all cases, which can be seen from the last step in the proof of the underlying Lemma 4, where the quantity $\#\{0 \le n < p_i \mid \mathbf{h}\cdot\mathbf{z}_n^{(i)} \equiv \mathbf{h}\cdot\mathbf{z}_k^{(i)} \pmod{p_i}\}$ is estimated by $B_i(\mathbf{h})$. In the full period case ($N = m$), another method of proof can be used, which allows to establish the following improved upper bounds depending on the quantities $A_i(\mathbf{h})$ instead of $B_i(\mathbf{h})$. These quantities also occur in the corresponding lower bounds for the discrepancy $D_{m;c_1,\ldots,c_r}^{(s)}$ in Theorems 5 and 6.

THEOREM 3. *The average value of the discrepancy $D_{m;c_1,\ldots,c_r}^{(s)}$ of s-dimensional vectors in the compound method over the parameters $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ satisfies*

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(c_1,\ldots,c_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{m;c_1,\ldots,c_r}^{(s)}\le\frac{s}{m}+\frac{1}{\sqrt{m}}\prod_{i=1}^{r}\sqrt{\frac{p_i}{p_i-1}}\\
&\quad\times\sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}}\prod_{i\in J}\sqrt{p_i-1}\sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\bmod p_i),i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\bmod p_i),i\notin J}}\frac{1}{r(\mathbf{h},m)}\prod_{\substack{i=1\\ i\notin J}}^{r}\sqrt{A_i(\mathbf{h})-1}.
\end{aligned}$$

Proof. First, it follows as in the proof of Theorem 1 (with $N = m$) that

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{m;c_1,\ldots,c_r}^{(s)}$$

$$\le \frac{s}{m} + \frac{1}{m} \sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}} \sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\, p_i),i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\, p_i),i\notin J}} \frac{1}{r(\mathbf{h},m)}$$

$$\times \sqrt{\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{m-1} e\left(\sum_{i=1}^{r} c_i(\mathbf{h}\cdot\mathbf{z}_n^{(i)})/p_i \right) \right|^2}.$$

Now, Lemma 5 is used instead of Lemma 4. This yields

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{m;c_1,\ldots,c_r}^{(s)} \le \frac{s}{m} + \frac{1}{\sqrt{m}} \prod_{i=1}^{r} \sqrt{\frac{p_i}{p_i-1}}$$

$$\times \sum_{\substack{J\subset\{1,\ldots,r\}\\ \#J<r}} \prod_{i\in J} \sqrt{p_i-1} \sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}(\mathrm{mod}\, p_i),i\in J\\ \mathbf{h}\not\equiv\mathbf{0}(\mathrm{mod}\, p_i),i\notin J}} \frac{1}{r(\mathbf{h},m)} \prod_{\substack{i=1\\ i\notin J}}^{r} \sqrt{A_i(\mathbf{h})-1},$$

which is the desired result. ■

THEOREM 4. *Let* $A_i = \max\{A_i(\mathbf{h}) \mid \mathbf{h}\in\mathbb{Z}^s, \mathbf{h}\not\equiv\mathbf{0}\ (\mathrm{mod}\ p_i)\}$ *for* $1 \le i \le r$. *Then the average value of the discrepancy* $D_{m;c_1,\ldots,c_r}^{(s)}$ *of s-dimensional vectors in the compound method over the parameters* $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ *satisfies*

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(c_1,\ldots,c_r)\in \mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{m;c_1,\ldots,c_r}^{(s)}$$

$$< \frac{1}{\sqrt{m}} \prod_{i=1}^{r} \left(\sqrt{\frac{p_i(A_i-1)}{p_i-1}} + \frac{1}{\sqrt{p_i}} \right) \left(\frac{2}{\pi}\log m + \frac{7}{5} \right)^s.$$

Proof. The desired estimate follows from Theorem 3 by the same arguments as in the proof of Theorem 2. ■

THEOREM 5. *Let* $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ *with* $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ *for* $1 \le i \le r$. *Then there exist parameters* $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ *such that the discrepancy* $D_{m;c_1,\ldots,c_r}^{(s)}$ *of s-dimensional vectors in the compound method satisfies*

$$D_{m;c_1,\ldots,c_r}^{(s)} \ge \frac{\pi}{2((\pi+1)^\ell - 1)\prod_{j=1}^s \max(1, |h_j|)} m^{-1/2} \prod_{i=1}^r \sqrt{\frac{p_i(A_i(\mathbf{h}) - 1)}{p_i - 1}},$$

where ℓ *denotes the number of nonzero coordinates of* $\mathbf{h}$.

Proof. First, Lemma 2 is applied with $N = m$, $k = s$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \le n < m$. This yields

$$\begin{aligned} D_{m;c_1,\ldots,c_r}^{(s)} &\ge \frac{\pi}{2m((\pi+1)^\ell - 1)\prod_{j=1}^s \max(1, |h_j|)} \left| \sum_{n=0}^{m-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \\ &= \frac{\pi}{2m((\pi+1)^\ell - 1)\prod_{j=1}^s \max(1, |h_j|)} \left| \sum_{n=0}^{m-1} e\left(\sum_{i=1}^r c_i(\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right| \end{aligned}$$

for any $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$. Now, Lemma 5 (with $J = \varnothing$) implies that there exist parameters $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ with

$$\left| \sum_{n=0}^{m-1} e\left(\sum_{i=1}^r c_i(\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right|^2 \ge m \prod_{i=1}^r \frac{p_i(A_i(\mathbf{h}) - 1)}{p_i - 1},$$

which yields the desired result. ■

THEOREM 6. *Let* $E_1, \ldots, E_r$ *be arbitrary integers with* $2 \le E_i < p_i$ *for* $1 \le i \le r$. *Then there exist parameters* $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ *and purely periodic sequences* $(\mathbf{z}_n^{(i)})_{n \ge 0}$ *of elements of* $\mathbb{Z}_{p_i}^s$ *with period length* p_i *and* $A_i(\mathbf{h}) \le B_i(\mathbf{h}) \le sE_i$ for all $\mathbf{h} \in \mathbb{Z}^s$ *with* $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ *and* $1 \le i \le r$ *such that the discrepancy* $D_{m;c_1,\ldots,c_r}^{(s)}$ *of the corresponding s-dimensional vectors in the compound method satisfies*

$$D_{m;c_1,\ldots,c_r}^{(s)} \ge \frac{1}{2\sqrt{2^r}} m^{-1/2} \prod_{i=1}^r \sqrt{E_i}.$$

Proof. First, for $1 \le i \le r$ and $0 \le n < p_i$, let $\mathbf{z}_n^{(i)} = (z_{n1}^{(i)}, \ldots, z_{ns}^{(i)}) \in \mathbb{Z}_{p_i}^s$ be defined by

$$z_{nj}^{(i)} \equiv (\lfloor n/E_i \rfloor + j - 1)^s \pmod{p_i}, \qquad 1 \le j \le s,$$

where $\lfloor x \rfloor$ means the greatest integer less than or equal to x. Now, for $1 \le i \le r$, a sequence $(\mathbf{z}_n^{(i)})_{n \ge 0}$ of elements of $\mathbb{Z}_{p_i}^s$ with period length p_i can be obtained by p_i-periodic continuation.

(i) Let $1 \le i \le r$ and $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ be fixed. Then

$$\mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv g(\lfloor n/E_i \rfloor) \pmod{p_i}, \quad 0 \le n < p_i,$$

where the polynomial $g: \mathbb{Z}_{p_i} \to \mathbb{Z}_{p_i}$ is given by

$$g(x) \equiv h_1 x^s + \cdots + h_s (x + s - 1)^s \pmod{p_i}.$$

First, suppose that $s < p_i$. Then straightforward arguments (e.g., the corresponding Vandermonde determinant is different from zero) show that $1 \le \deg(g) \le s$. Hence, for any $h_0 \in \mathbb{Z}_{p_i}$, the equation $g(x) = h_0$ has at most s different solutions, which implies that

$$\#\{0 \le n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv h_0 \pmod{p_i}\} \le sE_i$$

and therefore $A_i(\mathbf{h}) \le B_i(\mathbf{h}) \le sE_i$. On the other hand, if $s \ge p_i$, then the last estimate is trivial, since $A_i(\mathbf{h}) \le B_i(\mathbf{h}) \le p_i$ is always satisfied.

(ii) Now, let $1 \le i \le r$ and $\mathbf{h} = (1, 0, \ldots, 0) \in \mathbb{Z}^s$ be fixed. Since

$$\mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv (\lfloor n/E_i \rfloor)^s \pmod{p_i}, \quad 0 \le n < p_i,$$

it follows that

$$\begin{aligned} A_i(\mathbf{h}) &\ge \frac{1}{p_i} (\lfloor p_i/E_i \rfloor E_i^2 + (p_i - \lfloor p_i/E_i \rfloor E_i)^2) \\ &= E_i - \frac{1}{p_i} (p_i - \lfloor p_i/E_i \rfloor E_i) ((\lfloor p_i/E_i \rfloor + 1) E_i - p_i) \\ &\ge E_i - \frac{E_i^2}{4p_i} = \frac{p_i - 1}{2p_i} E_i + \frac{E_i(2p_i + 2 - E_i)}{4p_i} \ge \frac{p_i - 1}{2p_i} E_i + 1. \end{aligned}$$

Finally, Theorem 5 is applied with $\mathbf{h} = (1, 0, \ldots, 0) \in \mathbb{Z}^s$ (and $\ell = 1$). This yields

$$D_{m;c_1,\ldots,c_r}^{(s)} \ge \frac{1}{2} m^{-1/2} \prod_{i=1}^{r} \sqrt{\frac{p_i(A_i(\mathbf{h}) - 1)}{p_i - 1}} \ge \frac{1}{2\sqrt{2^r}} m^{-1/2} \prod_{i=1}^{r} \sqrt{E_i}$$

for some parameters $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$. ∎

Remark. The log-terms in the asymptotic behavior of the upper bounds can probably be improved if a general version of the Erdös–Turán–Koksma inequality is used instead of Lemma 1, but one has to pay the price of strongly increased absolute constants.

4. APPLICATION

The explicit inversive congruential method (with prime modulus) has been introduced in [4]. The compound version of this method is studied in [5, 8]. The following more general parallelized form of the explicit inversive congruential method is due to Niederreiter [17, 21].

For $1 \le i \le r$, let $a_{i1}, \ldots, a_{is} \in \mathbb{Z}_{p_i}^*$ and $b_{i1}, \ldots, b_{is} \in \mathbb{Z}_{p_i}$ be arbitrary fixed *parameters.* Let $z_{nj}^{(i)} \in \mathbb{Z}_{p_i}$ be defined by

$$z_{nj}^{(i)} \equiv (a_{ij} n + b_{ij})^{-1} \pmod{p_i}, \qquad n \ge 0, 1 \le j \le s,$$

where z^{-1} denotes the multiplicative inverse of $z \in \mathbb{Z}_{p_i}^*$ and $0^{-1} = 0$. It is obvious that the sequence $(\mathbf{z}_n^{(i)})_{n \ge 0}$ of elements of $\mathbb{Z}_{p_i}^s$ given by

$$\mathbf{z}_n^{(i)} = (z_{n1}^{(i)}, \ldots, z_{ns}^{(i)}), \qquad n \ge 0,$$

is purely periodic with period length p_i. Now, in the compound approach, the corresponding stream of s-dimensional vectors of (ordinary) *explicit inversive congruential pseudorandom numbers* is defined by

$$\mathbf{x}_n^{(i)} \equiv c_i \mathbf{z}_n^{(i)} / p_i \pmod{1}, \qquad n \ge 0,$$

where $c_i \in \mathbb{Z}_{p_i}^*$ is an additional *parameter.*

THEOREM 7. *Let $1 \le s \le \min\{p_1, \ldots, p_r\}$ and $1 \le N \le m$. For $1 \le i \le r$, let $a_{i1}^{-1} b_{i1}, \ldots, a_{is}^{-1} b_{is} \in \mathbb{Z}_{p_i}$ be distinct elements. Then the average value of the discrepancy $D_{N;c_1,\ldots,c_r}^{(s)}$ of s-dimensional vectors in the compound explicit inversive congruential method over the parameters $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ satisfies*

$$\frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1,\ldots,c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*} D_{N;c_1,\ldots,c_r}^{(s)} < \frac{1}{\sqrt{N}} \prod_{i=1}^r \frac{\sqrt{2sp_i} + 1}{\sqrt{p_i - 1}} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s.$$

Proof. For $1 \le i \le r$, it follows from [17, Theorem 1; 21, Theorem 1] that

$$\#\{0 \le n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv h_0 \pmod{p_i}\} \le 2s$$

for any $h_0 \in \mathbb{Z}_{p_i}$ and $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$. Hence, Theorem 2 can be applied with $B_i \le 2s$, which yields the desired result. ■

THEOREM 8. *Let $s \ge 2$. For $1 \le i \le r$, let $a_{i1} = a_{i2}$ and $b_{i1} \ne b_{i2}$ be fixed parameters. Then there exist $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ such that the discrepancy $D_{m;c_1,\ldots,c_r}^{(s)}$ of s-dimensional vectors in the compound explicit inversive congruential method satisfies*

$$D_{m;c_1,\ldots,c_r}^{(s)} \ge \frac{1}{2(\pi+2)}\, m^{-1/2}$$

for all parameters $a_{i3}, \ldots, a_{is} \in \mathbb{Z}_{p_i}^*$ and $b_{i3}, \ldots, b_{is} \in \mathbb{Z}_{p_i}$ with $1 \le i \le r$.

Proof. First, Theorem 5 is used with $\mathbf{h} = (1, -1, 0, \ldots, 0) \in \mathbb{Z}^s$. This implies that there exist $(c_1, \ldots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ with

$$D_{m;c_1,\ldots,c_r}^{(s)} \ge \frac{1}{2(\pi+2)}\, m^{-1/2} \prod_{i=1}^{r} \sqrt{\frac{p_i(A_i(\mathbf{h})-1)}{p_i-1}}.$$

Since $\mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv (a_{i1}n + b_{i1})^{-1} - (a_{i1}n + b_{i2})^{-1} \pmod{p_i}$, it follows that

$$A_i(\mathbf{h}) = \frac{1}{p_i} \sum_{h_0 \in \mathbb{Z}_{p_i}^*} (\#\{x \in \mathbb{Z}_{p_i} \mid (x+b_{i1})^{-1} - (x+b_{i2})^{-1} \equiv h_0 \pmod{p_i}\})^2.$$

Observe that $A_i(\mathbf{h}) = 2$ for $p_i = 2$, and assume from now on that $p_i \ge 3$. Then, $x \equiv -b_{i1} \pmod{p_i}$ and $x \equiv -b_{i2} \pmod{p_i}$ belong to $h_0 \equiv (b_{i1} - b_{i2})^{-1} \pmod{p_i}$, and all other values of $x \in \mathbb{Z}_{p_i}$ belong to a given $h_0 \in \mathbb{Z}_{p_i}^*$ if and only if

$$(2x + b_{i1} + b_{i2})^2 \equiv (b_{i2} - b_{i1})\,(b_{i2} - b_{i1} + 4h_0^{-1}) \pmod{p_i}.$$

Hence, $x \equiv -2^{-1}(b_{i1} + b_{i2}) \pmod{p_i}$ belongs to $h_0 \equiv 4(b_{i1} - b_{i2})^{-1} \pmod{p_i}$. Moreover, if $(b_{i2} - b_{i1})\,(b_{i2} - b_{i1} + 4h_0^{-1})$ is a quadratic residue modulo p_i for some other value of $h_0 \in \mathbb{Z}_{p_i}^*$, then there exist at least two different values of $x \in \mathbb{Z}_{p_i}$, which belong to this value of h_0. Therefore, the least possible value of $A_i(\mathbf{h})$ corresponds to the case that there exist exactly $(p_i - 1)/2$ different values of $h_0 \in \mathbb{Z}_{p_i}^*$ with exactly two different values of $x \in \mathbb{Z}_{p_i}$ belonging to each of them (and one remaining value of $x \in \mathbb{Z}_{p_i}$, namely $x \equiv -2^{-1}(b_{i1} + b_{i2}) \pmod{p_i}$, belonging to another value of $h_0 \in \mathbb{Z}_{p_i}^*$). This implies that

$$A_i(\mathbf{h}) \geq \frac{1}{p_i}\left(\frac{4(p_i-1)}{2}+1\right) = 2 - \frac{1}{p_i},$$

which completes the proof. ■

It should be observed that the upper bound in Theorem 7 is independent of the specific choice of the parameters in the compound explicit inversive congruential method. It applies for the full period ($N = m$) as well as for parts of the period ($N < m$), for equidistribution properties ($s = 1$) as well as for statistical independence properties ($s \geq 2$), and for the ordinary explicit inversive congruential method ($r = 1$) as well as for the compound approach ($r \geq 2$). For a fixed number r of prime factors of m, Theorem 7 shows that the discrepancy $D^{(s)}_{N;c_1,\ldots,c_r}$, on the average over the parameters $c_1, \ldots, c_r$, has an order of magnitude at most $N^{-1/2}(\log m)^s$. This order of magnitude fits well the probabilistic law of the iterated logarithm [1, 14] for the discrepancy of N true random points from $[0, 1)^s$, which is almost always of the order of magnitude $N^{-1/2}(\log\log N)^{1/2}$.

On the other hand, for dimensions $s \geq 2$, Theorem 8 shows that there exist parameters in the compound explicit inversive congruential method leading to a discrepancy $D^{(s)}_{m;c_1,\ldots,c_r}$ over the full period ($N = m$) of an order of magnitude at least $m^{-1/2}$.

Theorem 2 can also be applied to the (recursive) compound inversive congruential method and to the (general) compound nonlinear congruential method, which yields slightly improved versions of results in [10, 12], respectively.

ACKNOWLEDGMENT

The authors thank the referee for a valuable suggestion.

REFERENCES

1. K.-L. Chung, An estimate concerning the Kolmogoroff limit distribution, *Trans. Amer. Math. Soc.* **67** (1949), 36–50.
2. J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers: A tutorial, *Internat. Statist. Rev.* **60** (1992), 167–176.
3. J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers, *Z. Angew. Math. Mech.* **73** (1993), T644–T647.
4. J. Eichenauer-Herrmann, Statistical independence of a new class of inversive congruential pseudorandom numbers, *Math. Comp.* **60** (1993), 375–384.
5. J. Eichenauer-Herrmann, Explicit inversive congruential pseudorandom numbers: The compound approach, *Computing* **51** (1993), 175–182.

6. J. Eichenauer-Herrmann, On generalized inversive congruential pseudorandom numbers, *Math. Comp.* **63** (1994), 293–299.
7. J. Eichenauer-Herrmann, Compound nonlinear congruential pseudorandom numbers, *Monatsh. Math.* **117** (1994), 213–222.
8. J. Eichenauer-Herrmann, A unified approach to the analysis of compound pseudorandom numbers, *Finite Fields Appl.* **1** (1995), 102–114.
9. J. Eichenauer-Herrmann, Pseudorandom number generation by nonlinear methods, *Internat. Statist. Rev.* **63** (1995), 247–255.
10. J. Eichenauer-Herrmann and F. Emmerich, Compound inversive congruential pseudorandom numbers: An average-case analysis, *Math. Comp.* **65** (1996), 215–225.
11. J. Eichenauer-Herrmann and E. Herrmann, Compound cubic congruential pseudorandom numbers, *Computing,* to appear.
12. J. Eichenauer-Herrmann and G. Larcher, Average behaviour of compound nonlinear congruential pseudorandom numbers, *Finite Fields Appl.* **2** (1996), 111–123.
13. J. Eichenauer-Herrmann and G. Larcher, Average equidistribution properties of compound nonlinear congruential pseudorandom numbers, *Math. Comp.,* **66** (1997), 363–372.
14. J. Kiefer, On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm, *Pacific J. Math.* **11** (1961), 649–660.
15. H. Niederreiter, Recent trends in random number and random vector generation, *Ann. Oper. Res.* **31** (1991), 323–345.
16. H. Niederreiter, Nonlinear methods for pseudorandom number and vector generation, *in* "Simulation and Optimization" (G. Pflug and U. Dieter, Eds.), pp. 145–153, Lecture Notes in Economics and Math. Systems, Vol. 374, Springer-Verlag, Berlin, 1992.
17. H. Niederreiter, New methods for pseudorandom number and pseudorandom vector generation, *in* "Proc. 1992 Winter Simulation Conference" (J. J. Swain *et al.,* Eds.), pp. 264–269, IEEE Press, Piscataway, NJ, 1992.
18. H. Niederreiter, "Random Number Generation and Quasi-Monte Carlo Methods," SIAM, Philadelphia, PA, 1992.
19. H. Niederreiter, Finite fields, pseudorandom numbers, and quasirandom points, *in* "Finite Fields, Coding Theory, and Advances in Communications and Computing" (G. L. Mullen and P.J.-S. Shiue, Eds.), pp. 375–394, Dekker, New York, 1993.
20. H. Niederreiter, Pseudorandom numbers and quasirandom points, *Z. Angew. Math. Mech.* **73** (1993), T648–T652.
21. H. Niederreiter, On a new class of pseudorandom numbers for simulation methods, *J. Comput. Appl. Math.* **56** (1994), 159–167.
22. H. Niederreiter, New developments in uniform pseudorandom number and vector generation, *in* "Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing" (H. Niederreiter and P.J.-S. Shiue, Eds.), pp. 87–120, Lecture Notes in Statistics, Vol. 106, Springer-Verlag, New York, 1995.